

#5

Atty. Dkt. No. 074273/0179

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Yukiyasu TSUNOO

Title: ENCRYPTION EVALUATION
SUPPORT SYSTEM THAT CAN
LARGELY REDUCE EVALUATION
TIME OF ENCRYPTION
ALGORITHM, AND RECORD
MEDIUM RECORDING ITS
PROGRAM



Appl. No.: Unassigned

Filing Date: 1/23/2001

Examiner: Unassigned

Art Unit: Unassigned

CLAIM FOR CONVENTION PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application:

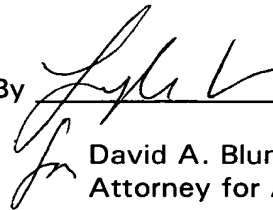
- Japanese Patent Application No. 2000-017878 filed January 24, 2000.

Respectfully submitted,

Date January 23, 2000

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5407
Facsimile: (202) 672-5399

By



David A. Blumenthal
Attorney for Applicant
Registration No. 26,257

LYLE KIMMS
REG. NO. 34079

74273/179
TSUNOO
I. 藤
US

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

2000年 1月24日

出 願 番 号
Application Number:

特願2000-017878

出 願 人
Applicant (s):

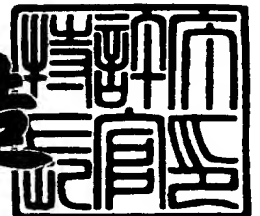
日本電気株式会社



2000年10月13日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3084399

【書類名】 特許願

【整理番号】 33509673

【提出日】 平成12年 1月24日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【発明者】

 【住所又は居所】 東京都港区芝五丁目7番1号 日本電気株式会社内

 【氏名】 角尾 幸保

【特許出願人】

 【識別番号】 000004237

 【氏名又は名称】 日本電気株式会社

【代理人】

 【識別番号】 100088959

 【弁理士】

 【氏名又は名称】 境 廣巳

【手数料の表示】

 【予納台帳番号】 009715

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9002136

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号評価支援システム及びプログラムを記録した機械読み取り可能な記録媒体

【特許請求の範囲】

【請求項 1】 予め定義した暗号アルゴリズム仕様記述法で記述された暗号アルゴリズムの図形表現を格納する評価対象記憶部と、

前記暗号アルゴリズム仕様記述法で使う単位図形の点数を記憶する点数記憶部と、

前記評価対象記憶部から図形表現を入力し、該図形表現中の単位図形に対して前記点数記憶部に記憶された点数を付与し、予め定められた計算ルールに従って前記図形表現全体の得点を計算して出力する評価実施手段とを備えた暗号評価支援システム。

【請求項 2】 前記評価実施手段が入力した図形表現中の利用者によって選択された単位図形を他の種類の単位図形に自動的に置き換えた図形表現を生成する自動組み替え手段を備え、前記評価実施手段は、前記入力した図形表現および前記自動組み替え手段で生成された図形表現について得点計算を行う請求項 1 記載の暗号評価支援システム。

【請求項 3】 前記点数記憶部は予め定められた複数の評価項目の各々についてその評価項目の得点計算に使用する各単位図形の点数を記憶しており、前記評価実施手段は、利用者から指定された評価項目毎に、前記点数記憶部に記憶された評価項目別の各単位図形の点数を参照して得点計算を行う請求項 1 または 2 記載の暗号評価支援システム。

【請求項 4】 前記複数の評価項目は、暗号強度に関する複数の評価項目を含む請求項 3 記載の暗号評価支援システム。

【請求項 5】 前記評価実施手段は、各評価項目毎に、前記図形表現中の信号の流れに沿って基本ブロックを通過する毎にその基本ブロックの点数を加点することで得点計算を行う請求項 4 記載の暗号評価支援システム。

【請求項 6】 前記点数記憶部に記憶される点数を単位図形のビット単位の点数とし、前記評価実施手段は、各評価項目毎に、前記図形表現の各出力ビット

毎の得点であるビット得点と、該ビット得点の平均値である項目得点とを算出する請求項 5 記載の暗号評価支援システム。

【請求項 7】 前記暗号アルゴリズム仕様記述法による暗号アルゴリズムの図形表現を利用者が記述および編集するのを支援する評価対象編集手段を備えた請求項 1、2、3、4、5 または 6 記載の暗号評価支援システム。

【請求項 8】 前記評価実施手段の計算結果を格納する評価結果記憶部と、該評価結果記憶部に格納された計算結果をグラフ化して出力する結果編集手段とを備えた請求項 1、2、3、4、5 または 6 記載の暗号評価支援システム。

【請求項 9】 前記評価実施手段の計算結果を格納する評価結果記憶部と、該評価結果記憶部に格納された計算結果を指定されたソートキーでソートして出力する結果編集手段とを備えた請求項 1、2、3、4、5 または 6 記載の暗号評価支援システム。

【請求項 10】 コンピュータを、
予め定義した暗号アルゴリズム仕様記述法による暗号アルゴリズムの図形表現を利用者が記述および編集するのを支援する評価対象編集手段、
該評価対象編集手段で編集された暗号アルゴリズムの図形表現を格納する評価対象記憶部、

前記暗号アルゴリズム仕様記述法で使う単位図形の点数を予め定められた複数の評価項目毎に記憶する点数記憶部、

前記評価対象記憶部に格納された図形表現を入力し、利用者から指定された評価項目毎に、図形表現中の単位図形に対して前記点数記憶部に記憶された当該評価項目にかかる点数を付与して予め定められた計算ルールに従って図形表現全体の得点を計算して出力する評価実施手段、

として機能させるプログラムを記録した機械読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は暗号アルゴリズムの評価作業を支援する暗号評価支援システムに関する。

【 0 0 0 2 】

【従来の技術】

ネットワークの急速な普及に伴い、情報の漏洩を防止する暗号技術の重要性が年々高まっている。暗号には大別して、暗号化と復号化で同じ鍵を使う共通鍵暗号と、秘密鍵と公開鍵という異なる鍵を使用する公開鍵暗号とがある。共通鍵暗号は送受信者間で鍵を共有する方法が問題となるが、公開鍵暗号に比べて暗号化及び復号化に要する計算量が少ない利点があるため、多くの分野や用途で使用されている。

【 0 0 0 3 】

他方、暗号アルゴリズムに対する解読技術も急速に進歩しており、利用している暗号の安全性が永久に保証されとは限られないのも事実である。従って、新しい解読技術に耐えられる新しい暗号アルゴリズムを積極的に設計し、事前にその強度を評価することが重要である。このための技術が従来より幾つか提案ないし実用化されている。

【 0 0 0 4 】

例えば、特開平 1 0 - 2 4 0 5 1 1 号公報（以下、文献 1 と称す）には、暗号アルゴリズムの設計を支援する従来技術の一例として、ビット列データを値とする変数のダイアグラム表現、ビット列データ上の演算のダイアグラム表現、変数と演算を組み合わせるためのダイアグラム表現といった所定のダイアグラム表現を使って、ブロック暗号アルゴリズム全体のダイアグラム表現をユーザが記述および編集できる暗号ダイアグラム編集装置が提案されている。また、同文献 1 には、暗号ダイアグラム編集装置を使って設計されたブロック暗号アルゴリズムからブロック暗号プログラムを自動的に生成する技術や、この生成されたプログラムが元のアルゴリズムを正確に実現しているか否かをテストする技術も提案されている。

【 0 0 0 5 】

他方、本出願人の先願にかかる特開平 1 1 - 2 1 2 4 5 2 号公報（以下、文献 2 と称す）には、開発された暗号プログラムの強度評価を支援する従来技術の一例として、多数の評価データ（平文、鍵等）を使って暗号プログラムの入出力デ

ータのビットごとの相関関係を統計的に求める手段と、求められたビットごとの相関関係を表形式やグラフ形式に編集して出力する手段とを備えた暗号強度評価支援装置が提案されている。

【0006】

【発明が解決しようとする課題】

文献1に示されるような暗号ダイアグラム編集装置を使えば暗号アルゴリズムの設計を効率化でき、また文献2に示されるような暗号強度評価支援装置を使えば暗号プログラムの強度評価をきめ細かく実施することができる。

【0007】

しかし、設計された暗号アルゴリズムの強度評価を実施するためには、暗号アルゴリズムから実際の暗号プログラムを生成した後、多数の評価データを使って統計的な処理を実行する必要がある、評価結果が出るまでに多くの時間を要する。1つの暗号アルゴリズムの設計から評価終了までの時間が長大化すると、限られた設計開発期間内で比較検討できる暗号アルゴリズム数、設計変更回数が限定され、利用目的に最適な暗号アルゴリズムを開発することが困難になる。

【0008】

そこで本発明の目的は、暗号アルゴリズムの評価時間を大幅に短縮し得る暗号評価支援システムを提供することにある。

【0009】

また本発明の別の目的は、暗号設計の専門家でなくても暗号アルゴリズムの評価を行うことができる暗号評価支援システムを提供することにある。

【0010】

【課題を解決するための手段】

本発明の暗号評価支援システムは、予め定義した暗号アルゴリズム仕様記述法で記述された暗号アルゴリズムの図形表現を格納する評価対象記憶部と、前記暗号アルゴリズム仕様記述法で使う単位図形の点数を記憶する点数記憶部と、前記評価対象記憶部から図形表現を入力し、該図形表現中の単位図形に対して前記点数記憶部に記憶された点数を付与し、予め定められた計算ルールに従って前記図形表現全体の得点を計算して出力する評価実施手段とを備えている。また、前記

評価実施手段が入力した図形表現中の利用者によって選択された単位図形を他の種類の単位図形に自動的に置き換えた図形表現を生成する自動組み替え手段を備え、前記評価実施手段は、前記入力した図形表現および前記自動組み替え手段で生成された図形表現について得点計算を行う構成も採用している。

【0011】

暗号アルゴリズムの設計及び評価に関する専門知識を有する技術者は、実際に設計した暗号アルゴリズムの構造と例えば文献2に見られるような暗号強度評価支援装置での評価結果との相関関係など、設計開発に必要な知見を有している。点数記憶部に記憶される各単位図形の点数は、そのような専門技術者の知見に基づいて設定されており、例えば暗号強度に関して良い傾向を持つと判断した単位図形には高い点数を、悪い傾向を持つと判断した単位図形には低い点数が付けられている。ここで、同じ単位図形であっても評価項目（例えばアバランシュ性評価、ビットバランス性評価など）が異なると傾向も異なる場合があるので、点数記憶部には予め定められた複数の評価項目別に単位図形の点数を記憶しておくのが望ましい。また、同じ単位図形であってもビット位置によって傾向も異なる場合があるので、点数はビット単位で設定するのが望ましい。この場合、評価実施手段は、例えば、各評価項目毎に、図形表現中の信号の流れに沿って基本ブロックを通過する毎にその基本ブロックの点数を加点することで、各評価項目毎に、例えば図形表現の各出力ビット毎の得点であるビット得点と、該ビット得点の平均値である項目得点とを算出する。

【0012】

また本発明の暗号評価支援システムは、前記暗号アルゴリズム仕様記述法による暗号アルゴリズムの図形表現を利用者が記述および編集するのを支援する評価対象編集手段、評価実施手段の計算結果を格納する評価結果記憶部、評価結果記憶部に格納された計算結果をグラフ化して出力する結果編集手段を備えることにより、暗号アルゴリズムの図形表現の編集からその得点計算、グラフ化による比較検討までの一連の作業を1つのシステムで支援可能としている。また、結果編集手段は、評価結果記憶部に格納された計算結果を指定されたソートキーでソートして出力する機能も備えており、複数の暗号アルゴリズムの優劣の判定をより

一層容易にしている。

【 0 0 1 3 】

【発明の実施の形態】

次に本発明の実施の形態の例について図面を参照して詳細に説明する。

【 0 0 1 4 】

図 1 を参照すると、本発明の一実施の形態にかかる暗号評価支援システム 1 0 は、データ処理装置 1 1 とそれに接続された表示装置 1 2、入力装置 1 3 および記憶装置 1 4 とを備えている。表示装置 1 2 は例えば L C D であり、入力装置 1 3 は例えばキーボード及びマウスである。記憶装置 1 4 は例えば磁気ディスク装置であり、データ処理装置 1 1 は例えば M P U 及び R O M や R A M 等で構成されたメモリを含むコンピュータ本体である。なお、印刷装置などその他の周辺装置が接続されていても良い。

【 0 0 1 5 】

データ処理装置 1 1 には、予め定義した暗号アルゴリズム仕様記述法による暗号アルゴリズムの図形表現（以下、関数ブロック図と称す）を利用者が記述および編集するのを支援する評価対象編集手段 1 1 1 と、関数ブロック図全体の得点を計算する評価実施手段 1 1 2 と、計算された得点を編集して出力する結果編集手段 1 1 3 とが設けられており、これらは G U I 1 1 4 を通じて表示装置 1 2 および入力装置 1 3 に接続されると共に、記憶インタフェース 1 1 5 を通じて記憶装置 1 4 に接続されている。また、関数ブロック図の一部を自動的に変更する自動組み替え手段 1 1 6 が評価実施手段 1 1 2 および記憶インタフェース 1 1 5 に接続されている。なお、本実施の形態では、共通鍵暗号を設計対象とするが、公開鍵暗号への適用も可能である。

【 0 0 1 6 】

他方、記憶装置 1 4 には、評価対象編集手段 1 1 1 で編集された関数ブロック図を格納する評価対象記憶部 1 4 1 と、暗号アルゴリズム仕様記述法で使う単位図形（以下、単位ブロックと称す）の各評価項目毎の点数を記憶する点数記憶部 1 4 2 と、評価実施手段 1 1 2 で計算された結果を格納する評価結果記憶部 1 4 3 と、自動組み替え手段 1 1 6 によって参照される置換部品一覧 1 4 4 とが設け

られている。

【0017】

利用者は、暗号評価支援システム10を用いて、

- (1) 関数ブロック図の編集
- (2) 関数ブロック図の得点計算
- (3) 計算結果の編集出力

の3つの作業を繰り返しながら、使用目的に合致する暗号アルゴリズムの開発を進めていく。関数ブロック図の編集(1)は暗号アルゴリズムの設計に相当し、主に評価対象編集手段111が支援する。関数ブロック図の得点計算(2)は暗号アルゴリズムの評価に相当し、主に評価実施手段112が支援する。計算結果の編集出力(3)は関数ブロック図の得点をグラフ化して出力するもので、結果編集手段113が支援する。以下、各場合に分けて、本実施の形態のより詳しい構成と動作を説明する。

【0018】

- (1) 関数ブロック図の編集

図2は評価対象編集手段111の処理例を示すフローチャートである。利用者が入力装置13から評価対象編集の開始を指示すると、評価対象編集手段111が起動され、図2に示す処理が実行される。まず、評価対象編集手段111は、関数ブロック図の新規編集か、過去に作成された関数ブロック図の更新かを、利用者の選択入力に応じて切りわけ(S11)。更新の場合には、利用者が入力装置13からファイル名で指定した関数ブロック図を記憶装置14の評価対象記憶部141から読み出し(S12)、この読み出した関数ブロック図を初期表示した編集ウィンドウを表示装置12に表示する(S13)。更新でなく新規作成の場合は、関数ブロック図が表示されていない編集ウィンドウを表示装置12に表示する(S13)。その後、利用者からの各種の編集操作に応答して、編集ウィンドウ上で編集処理を実行する(S14)。そして、編集作業の終了時、編集された関数ブロック図をファイルとして評価対象記憶部141に保存し(S15)、評価対象編集手段111は処理を終了する。

【0019】

図3に編集ウィンドウの構成例を示す。この例の編集ウィンドウ200は、タイトルバー201、メニューバー202、ツールバー203、ステータスバー204、関数ブロックウィンドウ300および基本ブロックバー400から構成されている。タイトルバー201には評価対象編集手段111の名前が表示される。メニューバー202には、「ファイル」、「編集」、「表示」、「挿入」などのメニュー項目が表示される。メニュー項目をマウスでクリックすると更にドロップダウンメニューが表示され、実行するコマンドを選択することができる。ツールバー203にはコマンドを表す一連のボタンが表示される。代表的なコマンドに、切取り、コピー、貼り付け、やり直し等の編集コマンドや、上書保存、新規作成などの他のコマンドがある。ステータスバー204にはコマンドの説明やキーボード状態などが表示される。これらはWindows95等におけるものと同様のものである。

【0020】

他方、関数ブロックウィンドウ300は、関数ブロック図を作成するためのウィンドウであり、基本ブロックバー400は、基本ブロックのボタンを表示する部分である。利用者は、基本ブロックバー400上のボタンによって適宜に基本ブロックを選択し、関数ブロックウィンドウ300上の適所に配置していくことで、所望の関数ブロック図を関数ブロックウィンドウ300上に作成する。

【0021】

図4は関数ブロックウィンドウ300の構成例を示す。この例の関数ブロックウィンドウ300は、タイトルバー301、列番号ゲージ302、行番号ゲージ303、垂直スクロールバー304、水平スクロールバー305および関数ブロック表示領域306から構成されている。関数ブロック表示領域306は縦横の枠線によって多数のセルに区切られており、行番号ゲージ303にはセルの行番号が、列番号ゲージ302にはセルの行番号がそれぞれ表示される。垂直スクロールバー304は関数ブロックウィンドウ300に表示されている部分の垂直位置の調整に使用し、水平スクロールバー305は関数ブロックウィンドウ300に表示されている部分の水平位置の調整に使用する。

【0022】

関数ブロックウィンドウ300に表示されている何れかのセルをマウスでクリックすると、そのセルがアクティブセルとなる。図3の基本ブロックバー400上で基本ブロックのボタンをクリックすると、アクティブセルにその基本ブロックが入力される。既にアクティブセルに基本ブロックが入力されていた場合には新しい基本ブロックで上書きされる。アクティブセルに基本ブロックが入力された時、関数ブロックウィンドウ300にプロパティウィンドウが開かれ、アクティブセルに入力された基本ブロックの詳細情報が表示される。基本ブロックの詳細情報はプロパティウィンドウにて変更可能である。なお、入力済みの基本ブロックを選択して、そのプロパティウィンドウを開くこともできる。

【0023】

図5にプロパティウィンドウの構成例を示す。この例のプロパティウィンドウ500はライン（配線）を分岐する単位ブロックのものであり、その中央部に適用時の当該単位ブロックのイメージ501が表示され、その周囲に入出力のデータ幅定義用エディットボックス502が配置されている。また、上部には0°、90°、180°、270°の4種類の回転ボタン503が設けられており、何れかの回転ボタン503が操作されると、イメージ501がそれに応じて変化する。当該基本ブロックの詳細情報を変更するには、回転ボタン503、データ幅定義用エディットボックス502で回転角や入出力のデータ幅に変更を加えた後、適用ボタン504をクリックする。なお、方向キー代替ボタン505はキーボードの方向キーの代替としてアクティブセルの移動に使用される。

【0024】

図6に基本ブロックバー400上で選択可能な基本ブロックの一覧を示す。基本ブロックは以下のようなグループに大別される。

- (A) 接続用（単位ブロック401～411）
- (B) 算術演算用（単位ブロック412～414）
- (C) 論理演算用（単位ブロック415～417）
- (D) シフト用（単位ブロック418～419）
- (E) ローテイトシフト用（単位ブロック420～423）
- (F) その他（単位ブロック424～427）

【 0 0 2 5 】

接続用の単位ブロックは、更に以下のような種類に分類される。

○ライン；隣接する2つの基本ブロック間を同じデータ幅のラインで接続するための単位ブロックで、単位ブロック401～403がこれに属する。複数種類用意されているのは、任意の方向での接続を可能にするためである。それらのプロパティウインドウでは、回転角およびデータ幅が設定可能である。

○フォーク；同じデータ幅で2方向にラインを分岐するための単位ブロックで、単位ブロック404、405がこれに属する。2種類用意されているのは、任意の方向への分岐を可能にするためである。それらのプロパティウインドウでは、回転角およびデータ幅が設定可能である。

○クロス；2つのラインが交差する箇所に用いる単位ブロックで、単位ブロック406がこれに属する。そのプロパティウインドウでは、回転角およびデータ幅が設定可能である。

○パーティション；データ幅を分割して2方向にラインを分岐するための単位ブロックで、単位ブロック408、409がこれに属する。2種類用意されているのは、任意の方向への分岐を可能にするためである。それらのプロパティウインドウでは、回転角、入力ラインのデータ幅、各出力ライン毎のデータ幅が設定可能である。

○ジョイン；2ラインを1ラインに結合するための単位ブロックで、単位ブロック410、411がこれに属する。2種類用意されているのは、任意の方向からの結合を可能にするためである。それらのプロパティウインドウでは、回転角、各入力ライン毎のデータ幅、出力ラインのデータ幅が設定可能である。

【 0 0 2 6 】

算術演算用の単位ブロックとしては、加算用の単位ブロック412、減算用の単位ブロック413、乗算用の単位ブロック414が用意されている。加算と減算の単位ブロック412、413のプロパティウインドウでは、回転角およびデータ幅が設定可能である。乗算の単位ブロック414のプロパティウインドウでは、回転角、各入力のデータ幅、出力のデータ幅が設定可能である。

【 0 0 2 7 】

論理演算用の単位ブロックとしては、排他的論理和用の単位ブロック 4 1 5、論理積用の単位ブロック 4 1 6、論理和用の単位ブロック 4 1 7 が用意されている。それらのプロパティウィンドウでは、回転角およびデータ幅が設定可能である。

【0 0 2 8】

シフト用の単位ブロックとしては、左シフト用の単位ブロック 4 1 8、右シフト用の単位ブロック 4 1 9 が用意されている。それらのプロパティウィンドウでは、回転各、データ幅およびシフト量が設定可能である。

【0 0 2 9】

ローテイトシフト用の単位ブロックとしては、左ローテイトシフト用の単位ブロック 4 2 0、右ローテイトシフト用の単位ブロック 4 2 1、上入力ダイナミックローテイトシフト用の単位ブロック 4 2 2、下入力ダイナミックローテイトシフト用の単位ブロック 4 2 3 が用意されている。単位ブロック 4 2 0、4 2 1 と単位ブロック 4 2 2、4 2 3 の違いは、前者はシフト量が事前に設定された値で固定化されるのに対し、後者は隣接する単位ブロックからのデータがシフト量として入力される点である。左右ローテイトシフトの単位ブロック 4 2 0、4 2 1 のプロパティウィンドウでは、回転角、データ幅およびシフト量が設定可能である。上下入力ダイナミックローテイトシフトの単位ブロック 4 2 2、4 2 3 のプロパティウィンドウでは、回転角、データ幅、シフト量を与えるデータのデータ幅が設定可能である。

【0 0 3 0】

その他、複数ビットのデータを他の複数ビットデータに置き換える換字テーブル用の単位ブロック 4 2 4、ビット位置を入れ替える転置テーブル用の単位ブロック 4 2 5、定数用の単位ブロック 4 2 6、鍵用の単位ブロック 4 2 7 が用意されている。換字テーブルの単位ブロック 4 2 4 のプロパティウィンドウでは、回転角および入出力のデータ幅が設定可能である。転置テーブルの単位ブロック 4 2 5 のプロパティウィンドウでは、回転角、入出力のデータ幅および出力ビット位置に対応する入力ビット位置の設定が可能である。鍵と定数の単位ブロックのプロパティウィンドウでは、回転角が設定可能である。なお、本実施の形態にお

ける評価対象編集手段111は、暗号アルゴリズム中で実際に使う鍵や定数、転置テーブルの内容を編集する機能は省略しているが、そのような機能を評価対象編集手段111に組み込むようにしても良いのは勿論のことである。

【0031】

利用者は、以上のような基本ブロック401～427の配置やそのプロパティの調整等を複数回実行することで、関数ブロックウィンドウ300上に所望の関数ブロック図を作成する。作成した関数ブロック図の一例を図7に示す。入力を x 、出力を y とした場合、図7の関数ブロック図は以下の式に対応する。

$$y = (e \ll n_4) \odot (e \vee x)$$

ここで、 $e = \{(d \ll n_3) - d\}$ 、 $d = \{(b \ll n_2) \odot b\} + K$ 、 $b = (a \ll n_1) + C + x + K$ であり、 \odot は排他的論理和を、 \vee は論理和を、 \ll は左シフトを、 $n_1 \sim n_4$ は図7中に合計4個ある左シフトの単位ブロックのシフト量をそれぞれ示す。

【0032】

編集を終えた関数ブロック図は、利用者によって指定されたファイル名を付与されて、例えば{(セルの列番号、行番号)、基本ブロックの詳細情報}を1レコードとして、評価対象記憶部141に保存される。

【0033】

(2) 関数ブロック図の得点計算

図8は評価実施手段112の処理例を示すフローチャートである。利用者が入力装置13から評価実施の開始を指示すると、評価実施手段112が起動され、図8に示す処理が実行される。まず、評価実施手段112は、メインダイアログボックスを表示装置12に表示し(S21)、このメインダイアログボックスを通じて利用者から計算対象とする関数ブロック図、評価項目、自動組み替え機能の使用可否等を指定させ、関数ブロック図の読み込み等、必要な事前準備を実行する(S22)。

【0034】

図9にメインダイアログボックスの構成例を示す。この例のメインダイアログボックス600は、タイトルバー601、関数ブロック操作部602、評価項目

選択部603、結果表示領域604および終了ボタン605から構成されている。タイトルバー601には評価実施手段112の名前が表示される。評価項目選択部603には、予め定められた幾つかの評価項目を選択するためのボタンBが表示される。利用者はボタンBをクリックして評価項目を選択する。評価項目は同時に複数選択可能である。結果表示領域604は計算結果を表示する領域であり、終了ボタン605は評価実施の終了を指示するボタンである。

【0035】

関数ブロック操作部602には、評価を実施する関数ブロック図のファイル名を入力するエディットボックス606がある。利用者は入力装置13から直接にファイル名をエディットボックス606に入力できる他、参照ボタン607をクリックすれば評価対象記憶部141に保存されている関数ブロック図のファイル名の一覧が表示されるので、その中から選択して入力することも可能である。ファイル名の入力後に関数読み込みボタン608をクリックされると、評価実施手段112は評価対象記憶部141から該当する関数ブロック図を内部に読み込む。

【0036】

また関数ブロック操作部602には、自動組み替え機能のオン、オフボタン609があり、利用者が何れか一方を選択できるようになっている。自動組み替え機能をオンした場合、評価実施手段112は、エディットボックス606でファイル名が指定された関数ブロック図を図4の関数ブロックウィンドウと同様なウィンドウに展開した試行マス選択ウィンドウを表示装置12に表示し、利用者にその画面上で試行マスを選択させる。試行マスとは、自動組み替え対象となる単位ブロックが配置されているセルのことである。試行マスの選択は、置換元となる単位ブロックが配置されているセルを例えばクリックすることで可能である。評価実施手段112は、選択された試行マスに配置されている単位ブロックが他の単位ブロックに置き換え可能な単位ブロックであれば、その試行マスの選択を有効とし、他のブロックに置き換え不可能な単位ブロックであれば、その旨表示して利用者に他のセルの選択を促す。他の基本ブロックに置き換え可能か否かは、選択された試行マスに配置されている単位ブロックの種類をキーに置換部品一覧144を検索し、置き換え可能な単位ブロックが少なくとも1つ以上設定されて

いるか否かによって判断する。

【0037】

更に関数ブロック操作部602には、計算の実行開始を指示する計算実行ボタン610、計算結果を保存するファイル名を入力するエディットボックス611、その参照ボタン612と結果保存ボタン613とが設けられている。利用者は入力装置13から直接にファイル名をエディットボックス611に入力できる他、参照ボタン612をクリックすれば評価結果記憶部143に保存されている評価結果ファイル名の一覧が表示されるので、その中から選択して入力することも可能である。ファイル名の入力後に結果保存ボタン613をクリックされると、評価実施手段112は計算結果を該当するファイルに保存する。

【0038】

評価実施手段112は、評価対象とする関数ブロック図の読み込み、自動組み替え機能のオン、オフの設定および評価項目の選択が完了した後、計算実行ボタン610をクリックされると、自動組み替え機能がオンの場合とオフの場合とで処理を切りわけ（図8のS23）。以下、各場合に分けて説明する。

【0039】

○自動組み替え機能オフの場合

評価実施手段112は、選択された評価項目の1つに注目し（S24）、点数記憶部142中の当該評価項目にかかる各単位図形の点数を参照して、評価対象とする関数ブロック図の当該評価項目にかかる得点を計算する（S25）。得点の計算方法については後述する。1つの評価項目の得点を計算すると、選択された評価項目の残りの1つに注目を移し（S26、S27）、同様の処理を繰り返す。以下、選択された全ての評価項目について、評価対象関数ブロック図の得点を計算する。

【0040】

○自動組み替え機能オンの場合

評価実施手段112は、評価対象とする関数ブロック図と試行マスの情報とを自動組み替え手段116に渡し、関数ブロック図の自動組み替えを実行させる（S28）。図10に自動組み替え手段116の処理例を示す。自動組み替え手段

116は、評価実施手段112から関数ブロック図と試行マスの情報とを入力すると（S51）、関数ブロック図上の試行マスに配置されている単位ブロックを識別し、その単位ブロックの種類をキーに置換部品一覧144を検索して、その単位ブロックと置換可能な単位ブロックを決定する（S52）。

【0041】

置換部品一覧144の一例を図11に示す。置換部品一覧144には、置き換え元となり得る単位ブロック毎に、置き換え可能な基本ブロックが記述されている。図11の場合、加算、減算、排他的論理和、論理積、論理和の基本ブロック412、413、415、416、417は相互に置換可能に指定されている。また左右シフトの単位ブロック418、419間、左右ローテイトシフトの単位ブロック420、421間、換字テーブル単位ブロック424と転置テーブル単位ブロック425間がそれぞれ置換可能に指定されている。

【0042】

自動組み替え手段116は、置換可能な単位ブロックを決定すると、関数ブロック図中の試行マスの単位ブロックを前記決定した単位ブロックで置き換えることにより、置換可能な単位ブロック毎の関数ブロック図を生成する（S53）。そして、生成した関数ブロック図を評価実施手段112に出力する（S54）。

【0043】

評価実施手段112は、自動組み替えが完了すると、利用者が評価対象として指定した関数ブロック図及び自動組み替え手段116で生成された関数ブロック図を評価対象関数ブロック図群とし、先ずその1つの関数ブロック図に注目する（S29）。次いで、ステップS24～S27と同様なステップS30～S33を実行することにより、当該関数ブロック図の各評価項目毎の得点を計算する。1つの関数ブロック図についての得点計算が終了すると（S33でYES）、評価対象関数ブロック図群の残り関数ブロック図の1つに注目を移し（S34）、その関数ブロック図の各評価項目毎の得点を計算する（S30～S33）。以下同様にして、評価対象関数ブロック図群の残りの関数ブロック図についても各評価項目毎の得点を計算する。

【0044】

以上のようにして関数ブロック図の得点計算が終了すると（S27またはS35でYES）、評価実施手段112は、計算結果を結果表示領域604に表示する（S36）。利用者は計算結果を保存する場合、前述したように結果ファイル名を指定して結果保存ボタン613をクリックすれば、計算結果が評価結果記憶部143に格納される（S37、S38）。なお、自動組み替え手段116がオンの場合、自動組み替え手段116で自動生成された関数ブロック図が、例えば生成元の関数ブロック図のファイル名の後ろに連番を付したファイル名で、評価対象記憶部141に自動的に格納される。

【0045】

次に関数ブロック図の得点計算について、基本ブロックの点数と得点計算方法とに分けて説明する。

【0046】

○基本ブロックの点数

点数記憶部142には、図12に示すように、各評価項目A、B、…、N毎に基本ブロックの点数がビット単位で設定されている。評価項目A、B、…、Nは、具体的には、アバランシュ性評価、入出力間関連性評価、出力ビット間関連性評価、ビットバランス性評価などの強度評価項目である。

【0047】

ここで、アバランシュ性評価とは、入力データに1ビットの変化を与えたときに出力ビットにどれだけ波及するかを評価するもので、入力の反転場所と出力の反転場所に有為な関係が存在せず、入力の反転ビット数と出力の反転ビット数に有為な関係が存在しない程、評価が高い。

【0048】

入出力ビット間関連性評価とは、入力データの各ビットと出力データの各ビットとの関連性を評価するもので、入力ビット値と有為な関係を持つ出力ビット値が存在しない程、評価が高い。

【0049】

出力ビット間関連性評価とは、出力データの各ビット間の関連性を評価するもので、どの出力ビット値どうしも有為な関係が存在しない程、評価が高い。

【0 0 5 0】

ビットバランス性評価とは、出力データの各ビットごとの1、0の出現頻度を評価するもので、入力値に依らずにどの出力ビットも0、1の出現比が1対1に近い程、評価が高い。

【0 0 5 1】

点数記憶部142において評価項目別に点数が設定されている理由は、同じ基本ブロックであっても評価項目が相違すれば暗号強度に及ぼす影響が異なる場合があり、その場合に付与する点数を相違させなければならないためである。例えば、論理和や論理積の基本ブロックは、ビットバランス性評価に関しては強度を弱める方向に作用することがあるが、出力ビット関連性評価に関しては強度変化に影響を与えず、アバランシュ性評価に関しては強度を強める方向に作用する。

【0 0 5 2】

また点数記憶部142において基本ブロックの点数をビット単位で設定する理由は、同じ基本ブロックであってもビット位置によって強度変化に及ぼす影響が異なる場合があるためである。例えば、アバランシュ性評価において、加算や減算の単位ブロックは、自出力ビット番号より下位の入力ビットが反転した場合、有為な関係が存在しないために強度を強めるように作用するので、自出力ビット番号より下位に入力ビットを持たない最下位1ビットとそれ以外のビットとは強度変化に及ぼす影響が相違する。

【0 0 5 3】

基本ブロックの各ビット毎の点数は、例えば、強度に変化が無い場合を0点とし、強くしている場合は正数、弱くしている場合は負数を与える。絶対値が大きいほどその度合いが大きいことを表す。具体的な点数の設定は、各評価項目毎に、基本ブロック間および基本ブロック内のビット間で比較し、評価経験に関する専門知識を有する者が当該評価項目に関して良い傾向を持つと判断したものには高い点数を、悪い傾向のものには低い点数を定義することで行う。なお、必ずしも全ての基本ブロックに点数を定義する必要はない。例えば、鍵や定数の基本ブロックへの点数の付与は省略できる。点数が定義されていない基本ブロックでは後述する加点はない。

【0054】

○得点の計算方法

ビット単位で持ち点を加点する。原則として入力ビットの得点（入力が複数ある場合はその総和）に、通過する基本ブロックの点数を加点する。単位ブロックの種類毎の加点方法の具体例を以下に示す。

【0055】

(a) 接続

(入力ビットの得点+点数)

(b) 加算、減算、論理和、論理積、排他的論理和

(同一入力ビット番号同士の得点の総和+点数)

(c) 乗算

(同一入力ビット番号同士の得点の総和を2倍の幅に広げたもの+点数)

ここで、2倍の幅に広げたものとは、同一入力ビット番号同士の得点の総和を、例えばx1, x2, x3, x4 (4ビットの場合) とすると、x1, x1, x2, x2, x3, x3, x4, x4である。

(d) シフト

(入力ビットの得点+点数) をシフト数に従って移動し、空いた出力ビットには0点を設定する。

(e) ローテイトシフト

(入力ビットの得点+点数) をシフト数に従って移動する。

(f) ダイナミックローテイトシフト

(入力ビットの最小点+シフトの最小点+点数) を計算し、全出力ビットの得点を置き換える。

(g) 換字

(入力ビットの得点+点数) を計算し、計算結果の最小点で全出力ビットの得点を置き換える。

(h) 転置

転置テーブルが定義されているときは、複数回出現するビットについては出現回数に応じて(入力ビットの得点+点数)を計算し、1回しか出現しないビット

についてはそのままテーブルに従って移動する。転置テーブルが定義されていないときは、（入力ビットの得点＋点数）を計算し、計算結果の最小点で全出力ビットの得点を置き換える。

【 0 0 5 6 】

例えば、入力ビット $a_0 \sim a_{31}$ と入力ビット $b_0 \sim b_{31}$ とを入力し、各ビット毎の論理和をとって出力ビット $c_0 \sim c_{31}$ を生成する論理和の基本ブロックにおいて、当該基本ブロックのビット番号 0 の点数を「1」、入力ビット a_0 の得点を「3」、入力ビット b_0 の得点を「5」とした場合、出力ビット c_0 の得点は、 $3 + 5 + 1 = 9$ となる。この出力ビット c_0 が次の基本ブロックの入力ビット d_0 となる場合、その入力ビット d_0 は「9」の得点を持つものとして扱われる。

【 0 0 5 7 】

このように本実施の形態において、基本ブロックを通過する毎に持ち点を順次加算していく加点方式を採用したのは、計算が簡易であり、関数ブロック図 1 つ当たりの計算時間を短くするためである。勿論、本発明はこのような計算方法に限定されるものではない。

【 0 0 5 8 】

さて、以上のような計算方法により、本実施の形態では、1 つの関数ブロック図について、各評価項目ごとに以下のような得点が計算される。

- (a) ビット得点；関数ブロック図の出力における各出力ビットごとの得点。
- (b) 項目得点；ビット得点の平均値。
- (c) 関数ブロック得点；項目得点の総和。

ビット得点と項目得点は図 8 のステップ S 2 5、S 3 1 で計算され、関数ブロック得点はステップ S 3 6 の計算結果の表示時に計算される。

【 0 0 5 9 】

(3) 計算結果の編集出力

図 1 3 は結果編集手段 1 1 3 の処理例を示すフローチャートである。利用者が入力装置 1 3 から結果編集出力の開始を指示すると、結果編集手段 1 1 3 が起動され、図 1 3 に示す処理が開始される。結果編集手段 1 1 3 は、先ず、評価結果

記憶部 1 4 3 に格納された一連の結果ファイル群の中から編集出力したい結果ファイルを利用者に選択させる (S 6 1)。これはファイル名を利用者に直接入力させても良く、ファイル名一覧を表示装置 1 2 に表示して選択させるようにしても良い。1 つのファイルだけを選択することもでき、複数のファイルを選択することもできる。複数のファイルを選択した場合、同一グラフ上に複数の関数ブロック図の得点が表示されることになる。

【 0 0 6 0 】

次に結果編集手段 1 1 3 は、得点種別を利用者に選択させる (S 6 2)。ここで、得点種別には、ビット得点、項目得点がある。ビット得点を選択した場合、評価項目も併せて選択させる。

【 0 0 6 1 】

次に結果編集手段 1 1 3 は、グラフ形式を利用者に選択させる (S 6 3)。これは、例えばグラフ形式の一覧を表示装置 1 2 に表示し、その中から利用者に所望のものを選択させるようにして良い。グラフ形式には、レーダーチャート、折れ線グラフ等の複数の形式が用意されている。

【 0 0 6 2 】

結果ファイル及びグラフ形式が決定すると、結果編集手段 1 1 3 は、該当する結果ファイルの評価結果記憶部 1 4 3 から読み込み、決定したグラフ形式のグラフを作成し (S 6 4)、表示装置 1 2 に表示する (S 6 5)。印刷装置がある場合、プリントアウトさせることも可能である。

【 0 0 6 3 】

図 1 4 および図 1 5 に表示装置 1 2 に表示されるグラフの例を示す。図 1 4 では、複数の関数ブロック図 X、Y、Z の各評価項目 A、B、…、毎の項目得点がレーダーチャート形式で表示されている。一般に面積が大きくなるほど良い傾向となるので、複数の関数ブロック図の比較を容易に行うことができる。また、個々の関数ブロック図についても評価項目どうしの関連を調べることによって、設計した暗号アルゴリズムの良否を判断できる。

【 0 0 6 4 】

図 1 5 は複数の関数ブロック図 X、Y、Z の或る評価項目 A についての出力ビ

ット毎の得点が折れ線グラフ形式で表示されている。横軸が出力ビット、縦軸がビット得点である。一般にグラフが上方向に推移するほど良い傾向となるので、複数の関数ブロック図の比較を容易に行うことができる。また、個々の関数ブロック図についても、出力ビットどうしの関連を調べることによって、設計した暗号アルゴリズムの良否を判断できる。

【0065】

また、本実施の形態の結果編集手段113は、複数の関数ブロック図をその得点によってソートする機能も有している。図16にその処理例を示す。利用者が入力装置13からソートの開始を指示すると、結果編集手段113が起動され、図16に示す処理が開始される。結果編集手段113は、先ず、評価結果記憶部143に格納された一連の結果ファイル群の中からソートしたい複数の結果ファイルを利用者に選択させる（S71）。これはファイル名を利用者に直接入力させても良く、ファイル名一覧を表示装置12に表示して選択させるようにしても良い。

【0066】

次に結果編集手段113は、ソートキーに使う評価項目を利用者に選択させる（S72）。ソートキーは、第1ソートキーから第mソートキーまで最大mレベル指定でき、利用者は暗号の用途などの設計要件に応じてソートキーの数と各レベル毎の評価項目を選択する。各レベルのソートキーとしてどの評価項目を使うかを外部ファイルに設定しておくことも可能であり、その場合は外部ファイルを選択すれば良い。

【0067】

結果ファイル及びソートキーが決定すると、結果編集手段113は、該当する結果ファイルの評価結果記憶部143から読み込み、より上位レベルのソートキーで指定された評価項目の得点（項目得点）が高くなる順序に結果ファイルを並べ替え（S73）、順位の高い順に結果ファイル名を並べたソート結果を表示装置12に表示する（S74）。印刷装置がある場合、プリントアウトさせることも可能である。

【0068】

以上のようなソート機能を使えば、例えば自動組み替え機能を使って或る単位ブロックを別の単位ブロックに置き換えて生成した複数の関数ブロック図（生成元の関数ブロック図を含む）の結果ファイルを選択し、得点計算時に指定した各評価項目をソートキーに指定したソートを行うことで、複数の関数ブロック図の優劣を容易に判断することが可能となる。勿論、自動組み替え機能で生成された関数ブロック図以外の複数の関数ブロック図のソートも可能である。

【 0 0 6 9 】

図 1 7 は本発明を適用したコンピュータの構成例を示す平面図である。コンピュータ 1 は、中央処理装置、主記憶等のメモリ、ハードディスク装置、フロッピィディスク装置、CD-ROM ユニットなどを備えるコンピュータ本体 2 と、表示装置 3 と、キーボード 4 と、マウス 5 とで構成される。6 はフロッピィディスク、CD-ROM 等の機械読み取り可能な記録媒体であり、暗号評価支援プログラムが記録されている。記録媒体 6 に記録された暗号評価支援プログラムは、コンピュータ本体 2 によって読み取られ、コンピュータ本体 2 の動作を制御することにより、コンピュータ本体 2 のメモリに評価対象記憶部 1 4 1、点数記憶部 1 4 2、評価結果記憶部 1 4 3 および置換部品一覧 1 4 4 をロードすると共に、コンピュータ本体 2 上に、評価対象編集手段 1 1 1、評価実施手段 1 1 2、結果編集手段 1 1 3、GUI 1 1 4、記憶インタフェース 1 1 5 および自動組み替え手段 1 1 6 を生成する。

【 0 0 7 0 】

以上本発明の実施の形態について説明したが、本発明は以上の実施形態にのみ限定されず、その他各種の付加変更が可能である。例えば評価項目としては主に統計的な暗号強度に関する評価項目を例示したが、線形解読法など攻撃に対する暗号強度に関する評価項目も同じ原理で適用可能である。また、設計した暗号アルゴリズムをソフトウェアやハードウェアで実行した場合の処理量や規模の見積もりにも同じ原理で適用可能である。また、複数の基本ブロックをユーティリティブロックとして、あたかも 1 つの基本ブロックのように扱えるマクロ機能を評価対象編集手段 1 1 1 に持たせるようにしても良い。

【 0 0 7 1 】

【発明の効果】

以上説明したように本発明によれば以下のような効果が得られる。

【0072】

暗号アルゴリズムの評価時間を大幅に短縮することができる。その理由は、文献2に記載の暗号強度評価支援装置のように実際の暗号プログラムを用いた統計的な処理が不要であり、暗号アルゴリズムの図形表現の段階で得点計算という非統計的な処理で評価結果が得られるためである。但し、本発明の暗号評価支援システムによる評価結果は文献2に記載の暗号強度評価支援装置による評価結果よりも正確さで劣るため、数多く設計した暗号アルゴリズムを先ず本発明の暗号評価支援システムで選別し、上位幾つかの暗号アルゴリズムを文献2に記載の暗号強度評価支援装置などを使ってより正確に評価することが必要である。

【0073】

暗号設計の専門家でなくても暗号アルゴリズムの評価を行うことができる。その理由は、得点という数値によって優劣を判断できるためである。また、複数の暗号アルゴリズムの優劣を得点の大小で判断できるためである。

【0074】

自動組み替え手段を持つ構成にあっては、多くの暗号アルゴリズムの設計と評価を効率良く実施することができる。その理由は、指定した図形単位を他の図形単位に置き換えた図形表現が自動的に作成されるからである。

【0075】

グラフ化機能を持つ結果編集手段を備えた構成にあっては、得点をグラフ化できるため優劣を直感的に把握でき、またソート機能を持つ結果編集手段を備えた構成にあっては、複数の暗号アルゴリズムを自動的に順序付けることができる。

【図面の簡単な説明】

【図1】

本発明の一実施の形態にかかる暗号評価支援システムのブロック図である。

【図2】

評価対象編集手段の処理例を示すフローチャートである。

【図3】

編集ウィンドウの構成例を示す図である。

【図 4】

関数ブロックウィンドウの構成例を示す図である。

【図 5】

プロパティウィンドウの構成例を示す図である。

【図 6】

基本ブロックバー上で選択可能な基本ブロックの一覧を示す図である。

【図 7】

関数ブロック図の一例を示す図である。

【図 8】

評価実施手段の処理例を示すフローチャートである。

【図 9】

メインダイアログボックスの構成例を示す図である。

【図 1 0】

自動組み替え手段の処理例を示すフローチャートである。

【図 1 1】

置換部品一覧の一例を示す図である。

【図 1 2】

点数記憶部の構成例を示す図である。

【図 1 3】

結果編集手段の処理例を示すフローチャートである。

【図 1 4】

表示装置に表示されるグラフの例を示す図である。

【図 1 5】

表示装置に表示されるグラフの他の例を示す図である。

【図 1 6】

結果編集手段の他の処理例を示すフローチャートである。

【図 1 7】

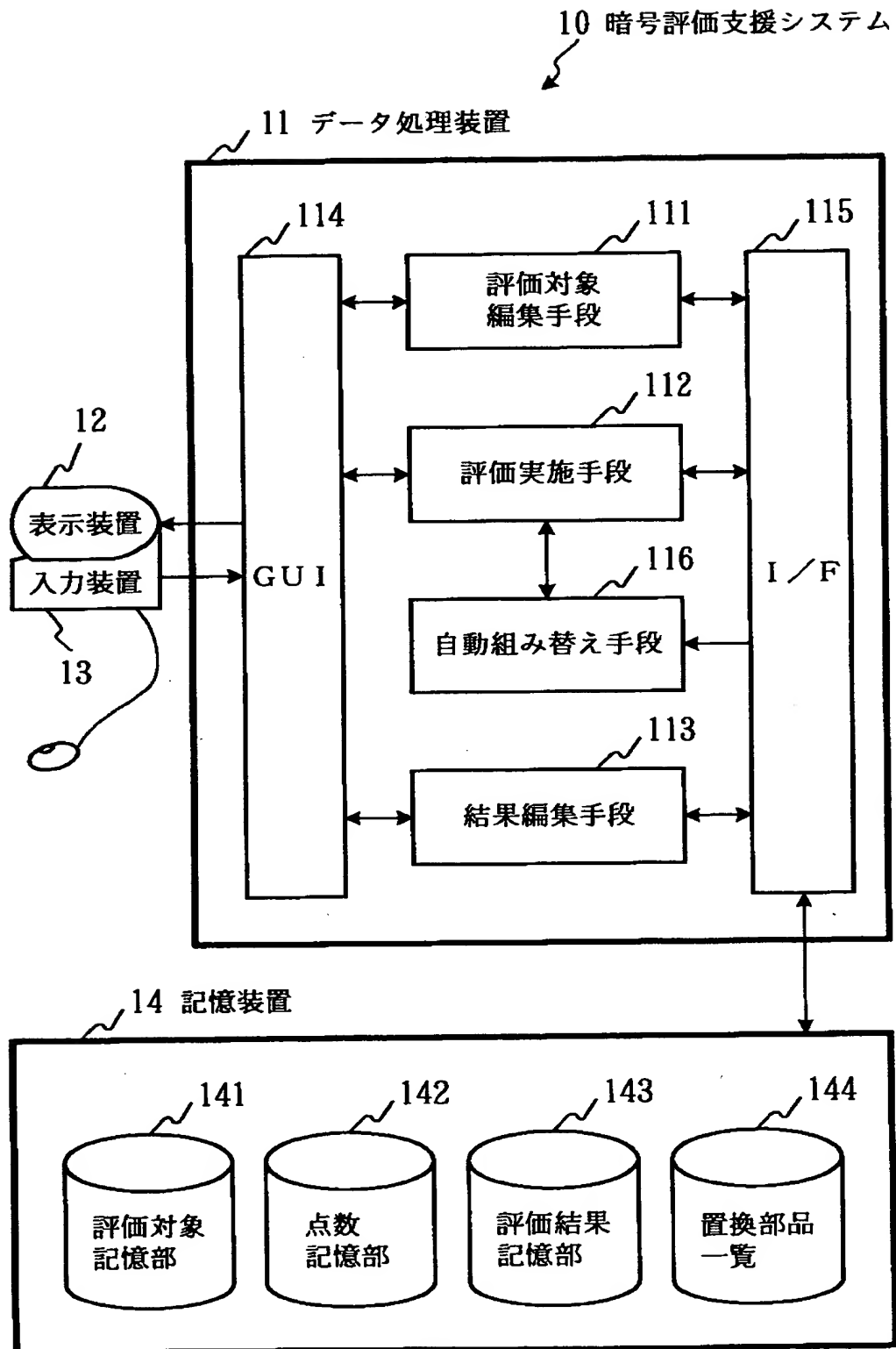
本発明を適用したコンピュータの構成例を示す平面図である。

【符号の説明】

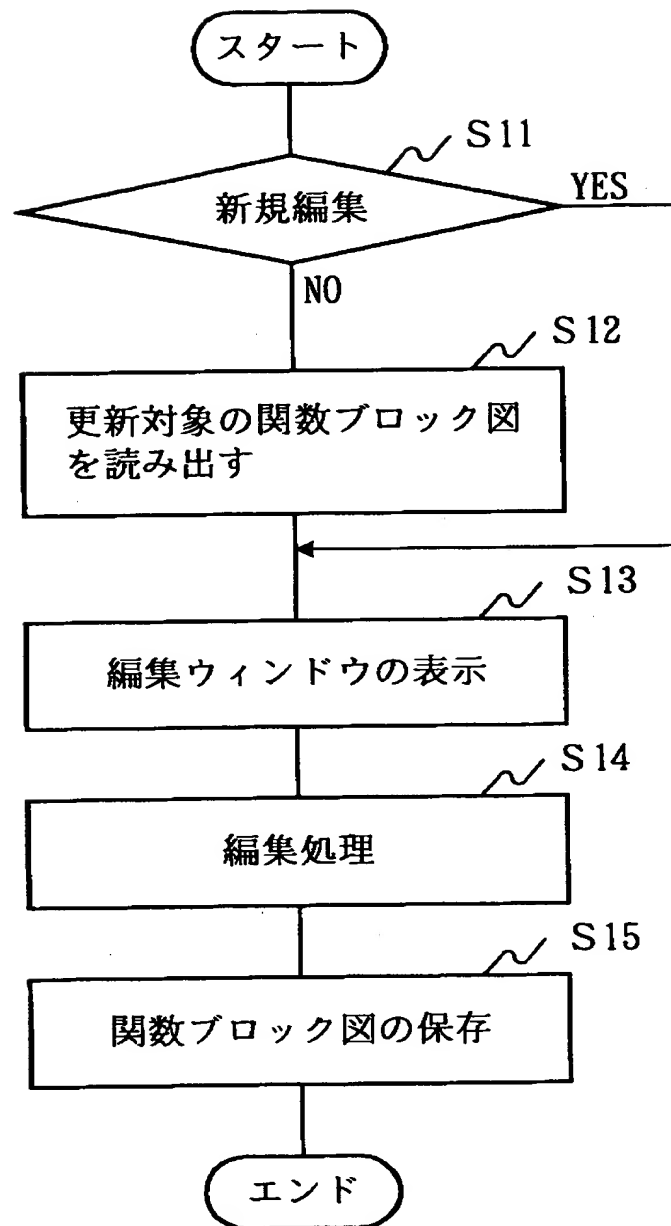
- 1 0 …暗号評価支援システム
- 1 1 …データ処理装置
 - 1 1 1 …評価対象編集手段
 - 1 1 2 …評価実施手段
 - 1 1 3 …結果編集手段
 - 1 1 4 …G U I
 - 1 1 5 …記憶インタフェース
 - 1 1 6 …自動組み替え手段
- 1 2 …表示装置
- 1 3 …入力装置
- 1 4 …記憶装置
 - 1 4 1 …評価対象記憶部
 - 1 4 2 …点数記憶部
 - 1 4 3 …評価結果記憶部
 - 1 4 4 …置換部品一覧

【書類名】 図面

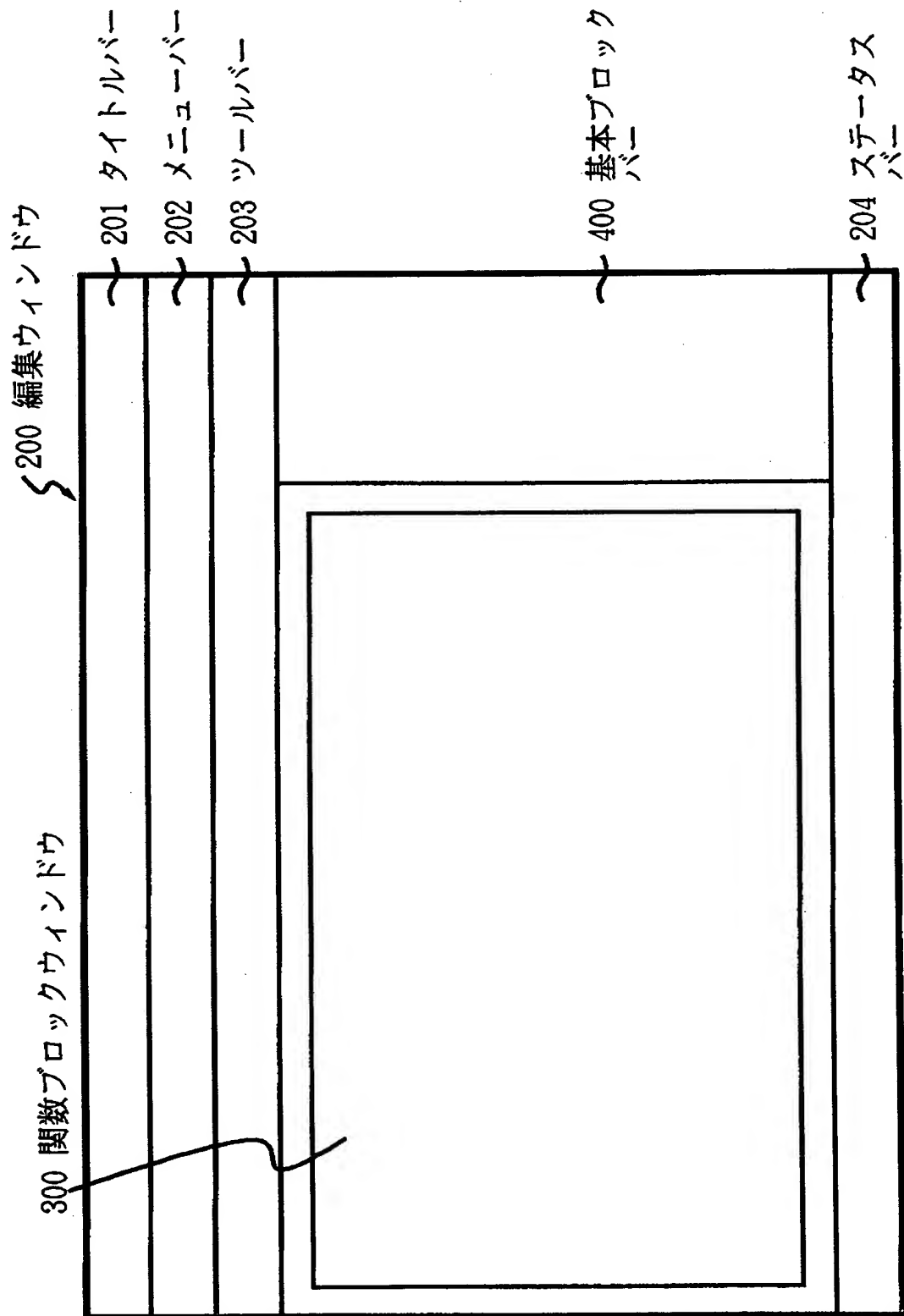
【図 1】



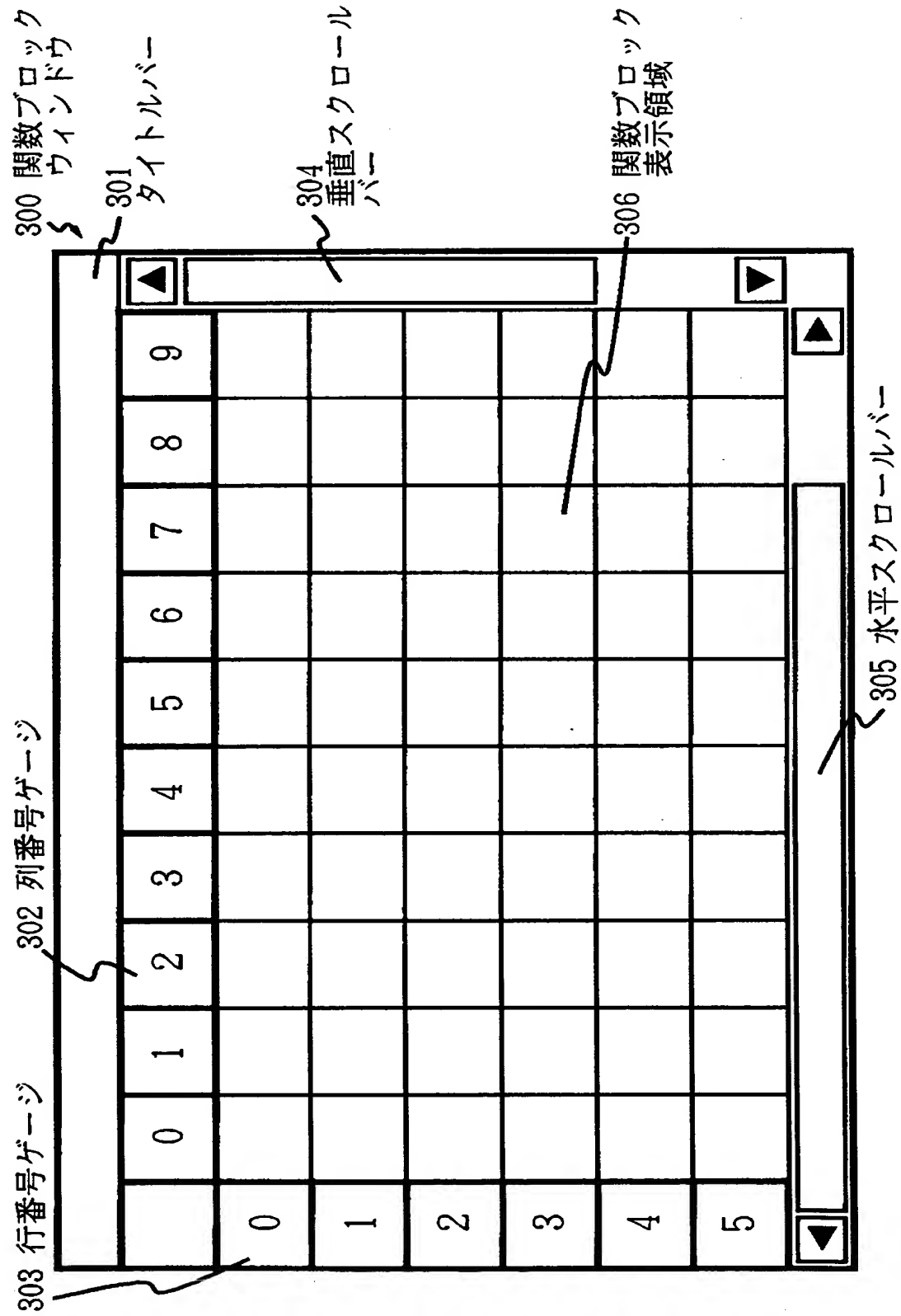
【図2】



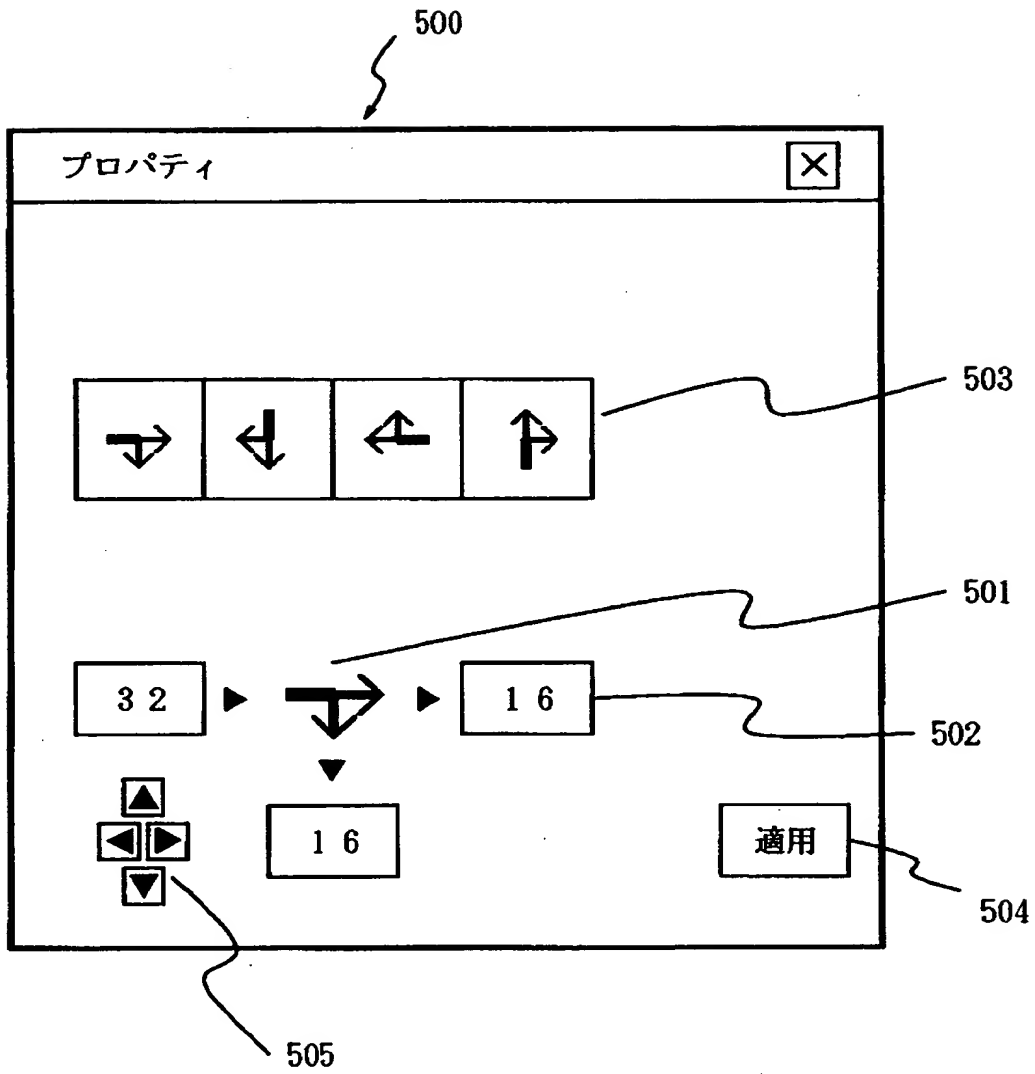
【図3】



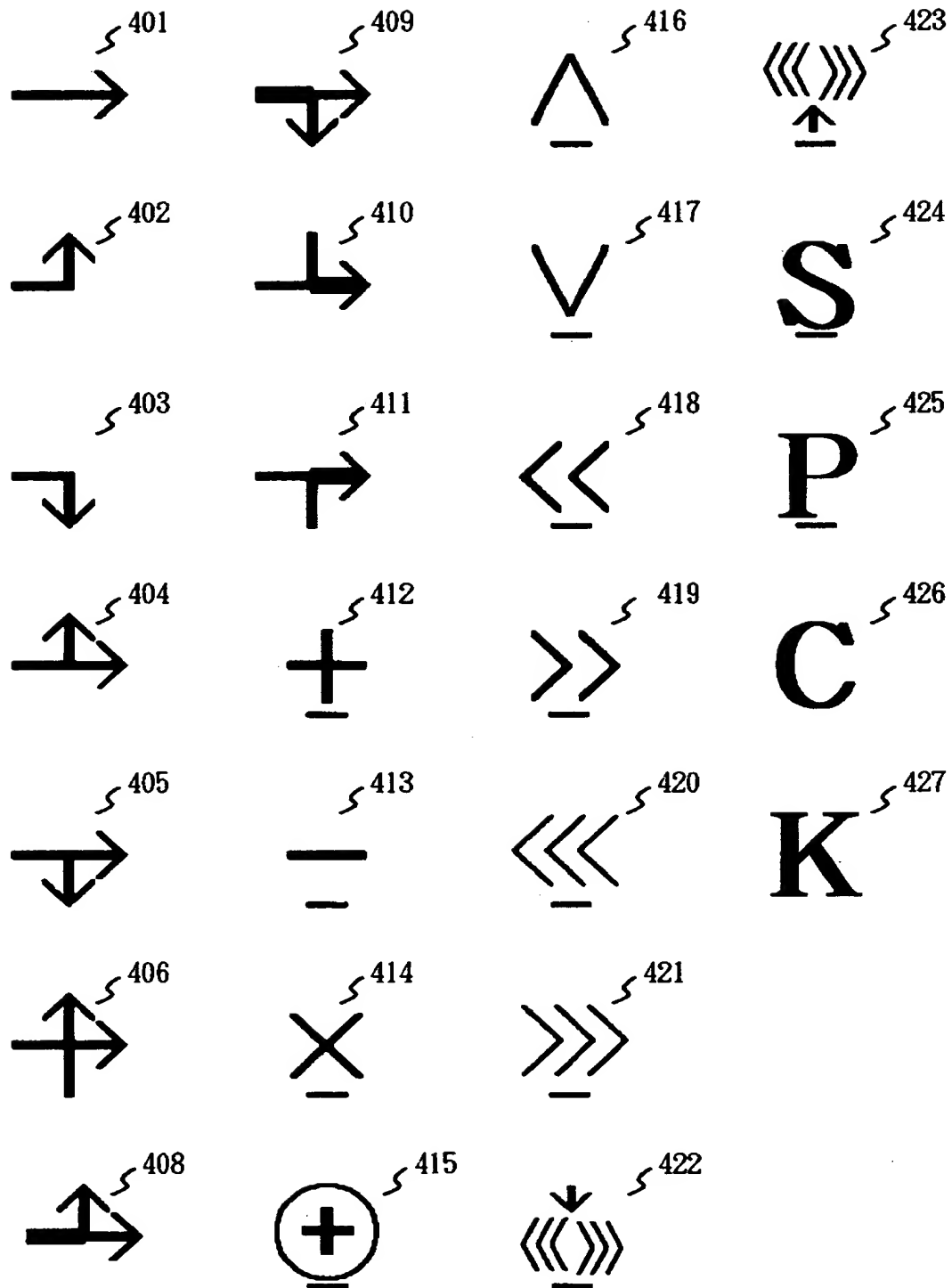
【図 4】



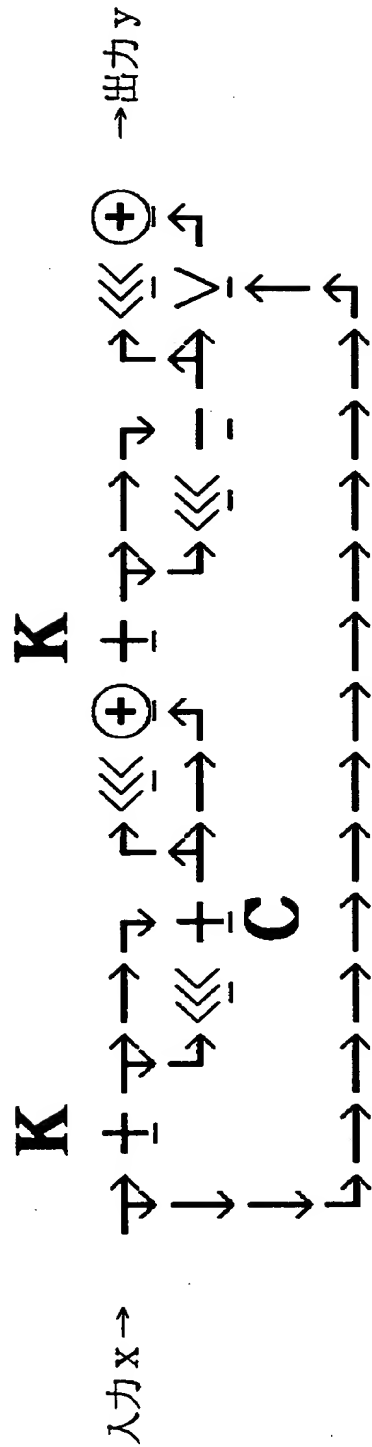
【図 5】



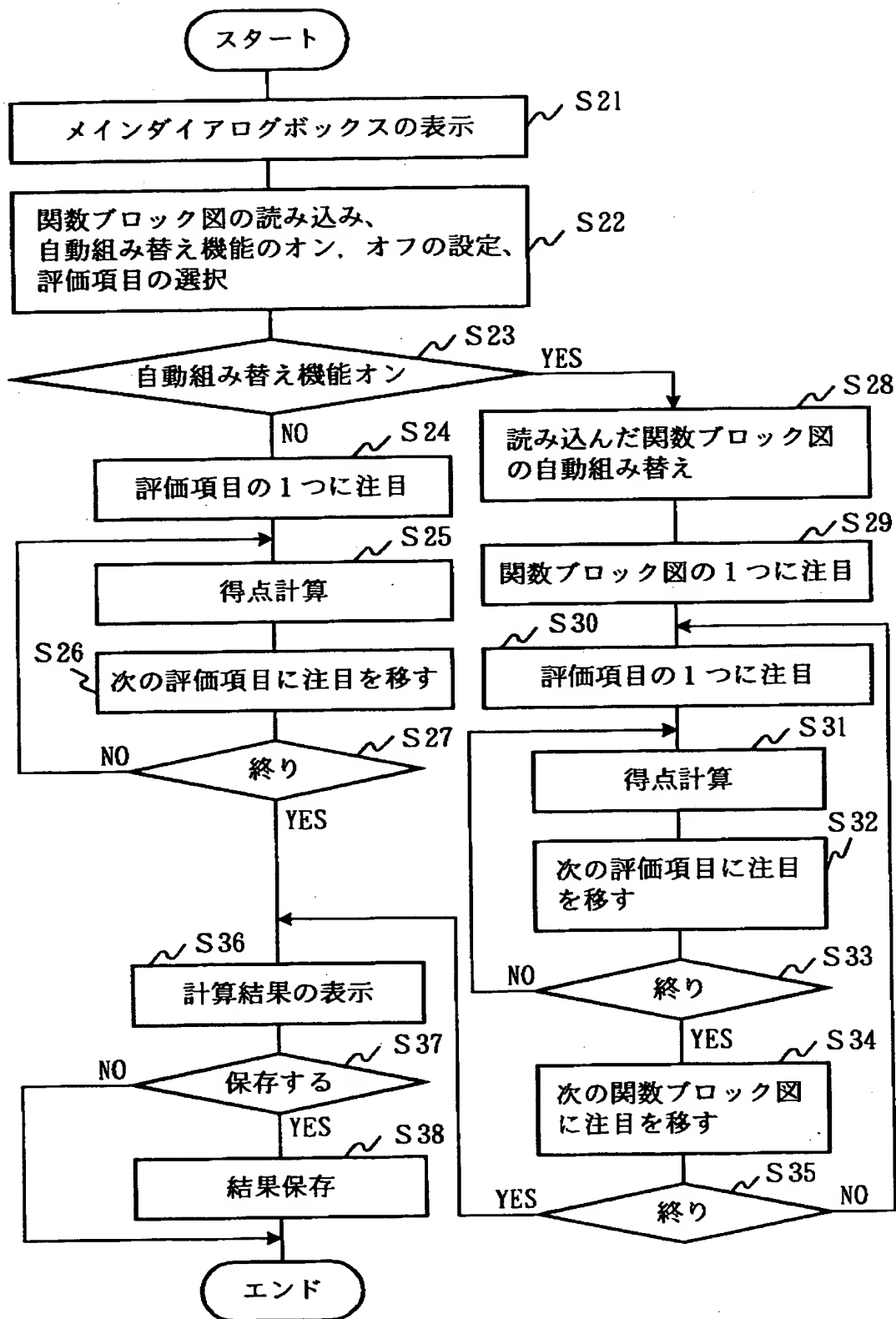
【図 6】



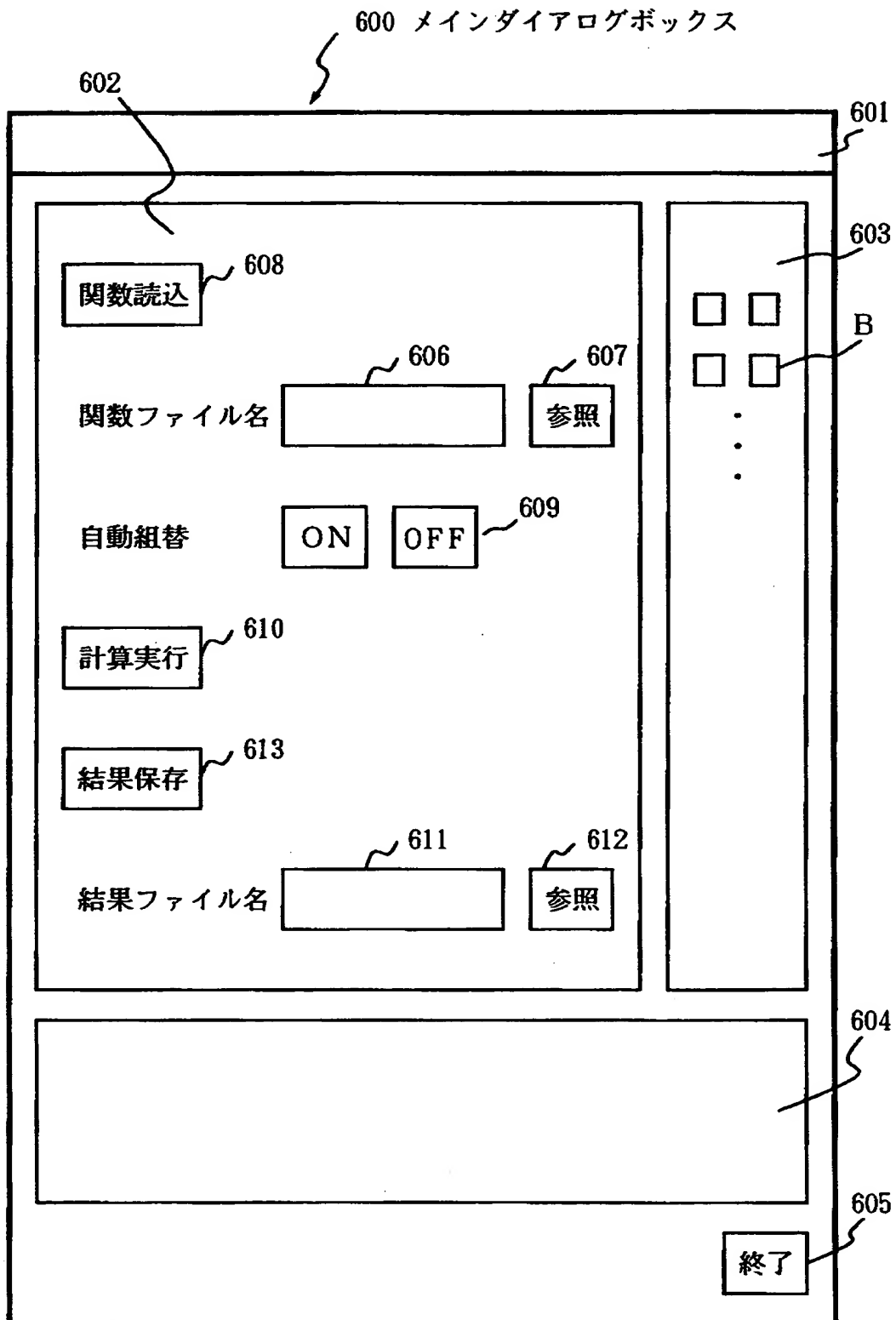
【図 7】



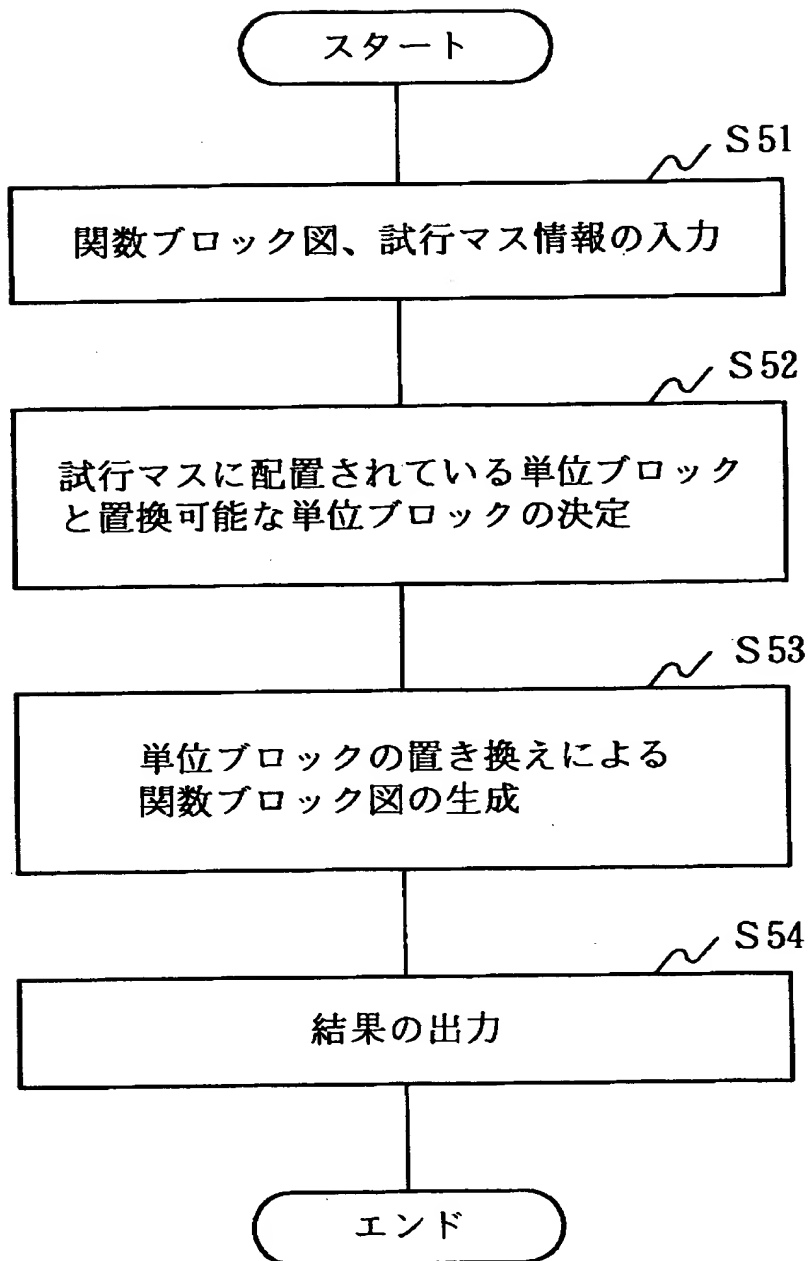
【図 8】



【図 9】



【図10】



【図 1 1】

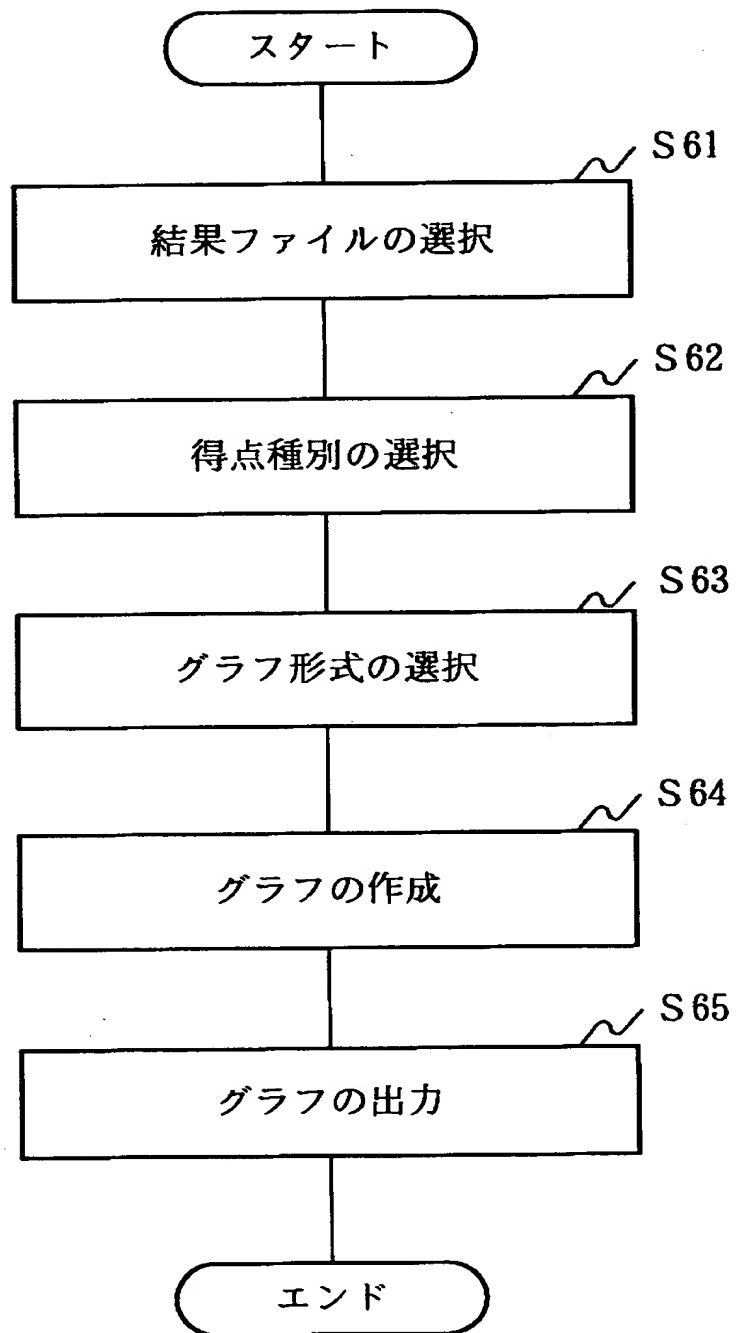
144 置換部品一覧

置き換え元	置き換え可能な基本ブロック
基本ブロック412	基本ブロック413、415、416、417
基本ブロック413	基本ブロック415、416、417、412
基本ブロック415	基本ブロック416、417、412、413
基本ブロック416	基本ブロック412、413、415、417
基本ブロック417	基本ブロック416、412、413、415
基本ブロック425	基本ブロック424
基本ブロック424	基本ブロック425
基本ブロック418	基本ブロック419
基本ブロック419	基本ブロック418
基本ブロック420	基本ブロック421
基本ブロック421	基本ブロック420

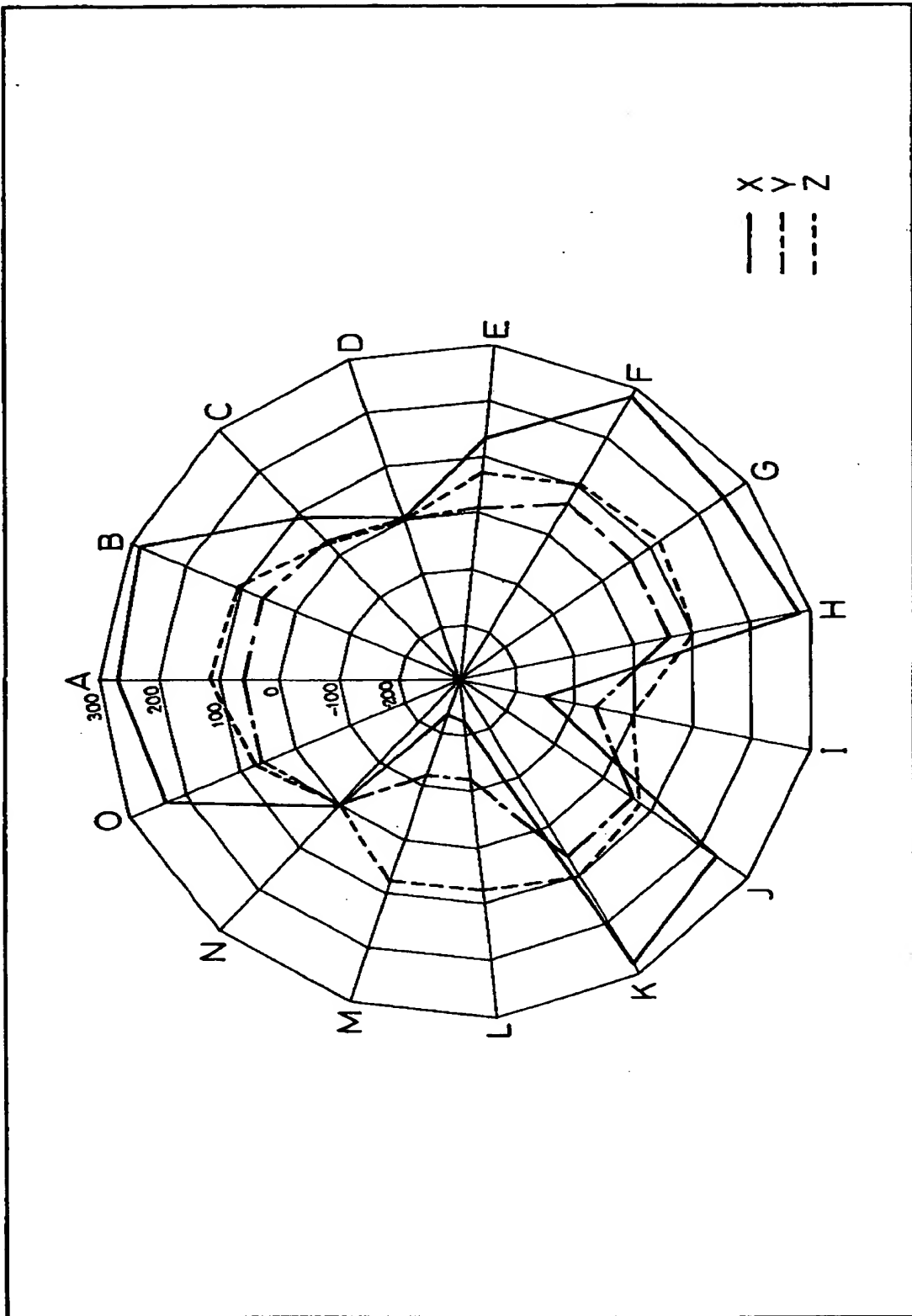
【図 1 2】

評価項目	基本ブロックの点数
A	
B	
⋮	
N	

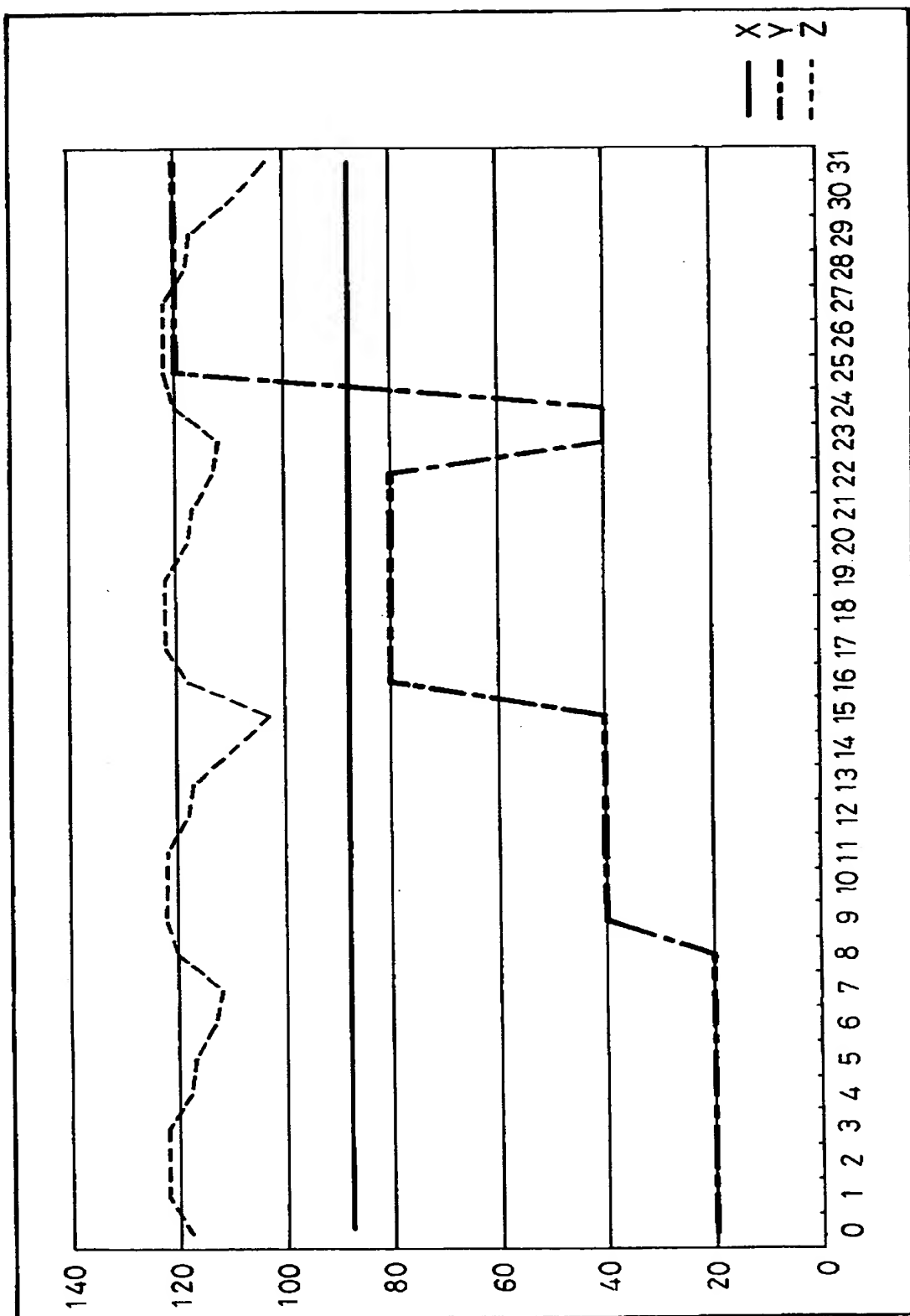
【図13】



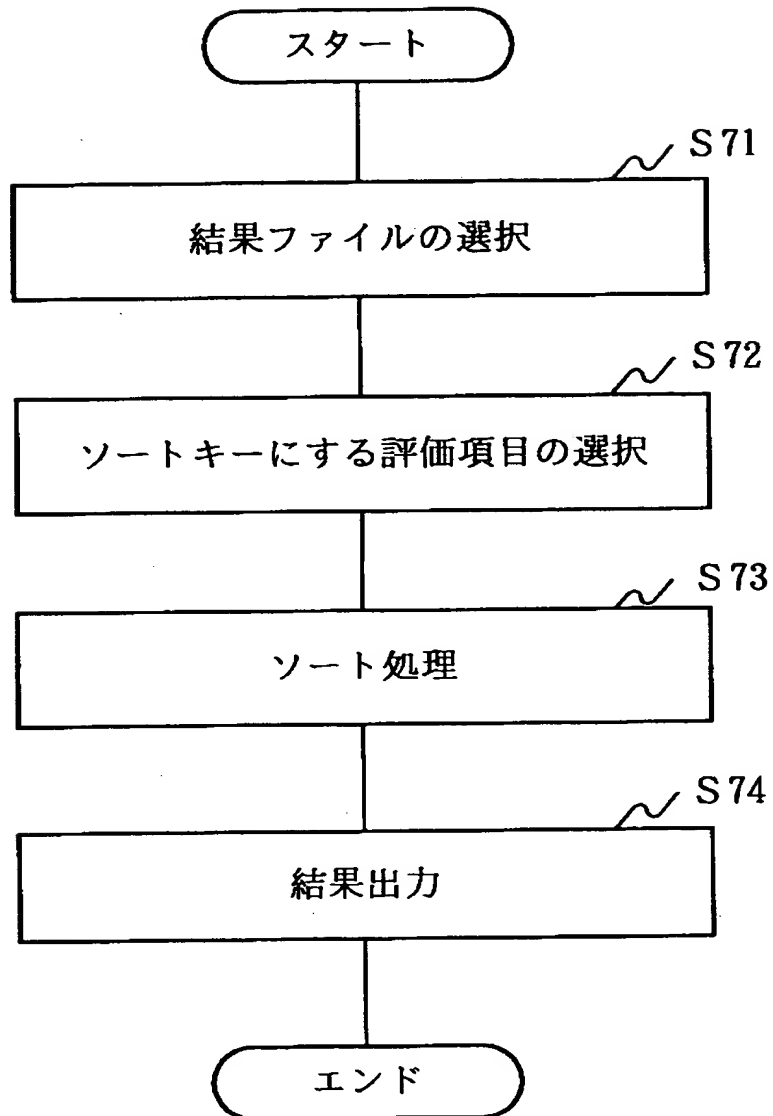
【図14】



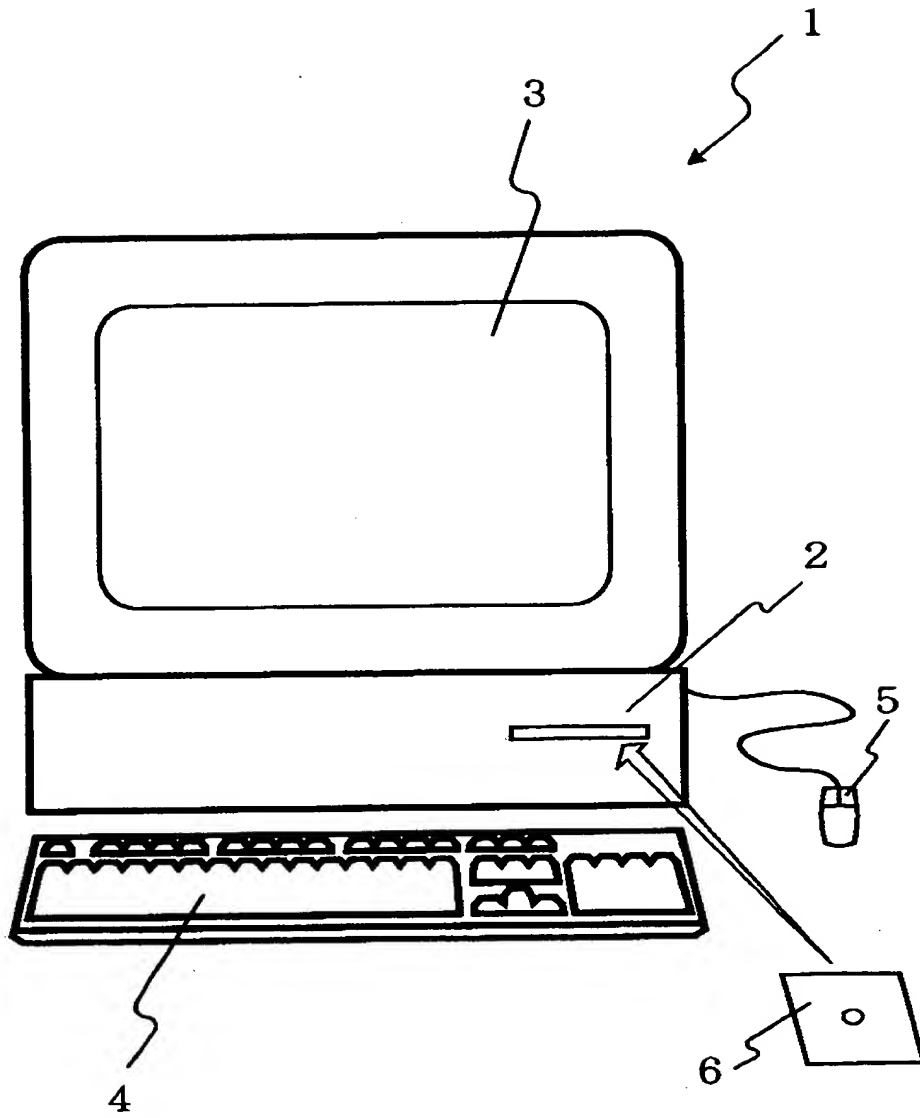
【図15】



【図16】



【図17】



【書類名】 要約書

【要約】

【課題】 暗号アルゴリズムの評価時間を大幅に短縮でき、かつ暗号設計の専門家でなくても強度評価などが行える暗号評価支援システムを提供する。

【解決手段】 点数記憶部142 には、予め定義した暗号アルゴリズム仕様記述法で使う単位図形の点数が暗号設計と評価の専門家の知識と経験をもとに事前に設定されている。評価対象記憶部141 には、前記暗号アルゴリズム仕様記述法で記述された暗号アルゴリズムの図形表現（関数ブロック図）が格納される。入力装置13からの利用者の指定に従い、評価実施手段112 は、評価対象記憶部141 から関数ブロック図を入力し、その中の単位図形に対して点数記憶部142 に記憶された点数を付与し、予め定められた計算ルールに従って関数ブロック図全体の得点を計算して表示装置12に出力する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000004237]

1. 変更年月日	1990年 8月29日
[変更理由]	新規登録
住 所	東京都港区芝五丁目7番1号
氏 名	日本電気株式会社